RSAC 2025 Conference

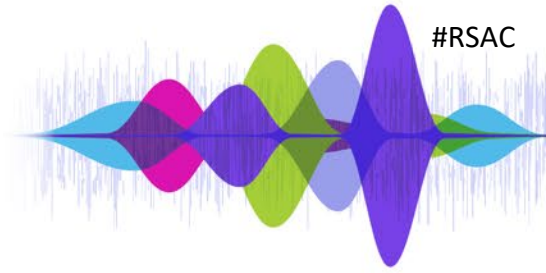
Many Voices.
One Community.

SESSION ID: GRC-R01

Architecting Data Analytics for Continuous Risk Management

James Tarala

Senior Instructor, the SANS Institute
Managing Partner, Cyverity
https://www.linkedin.com/in/jamestarala/

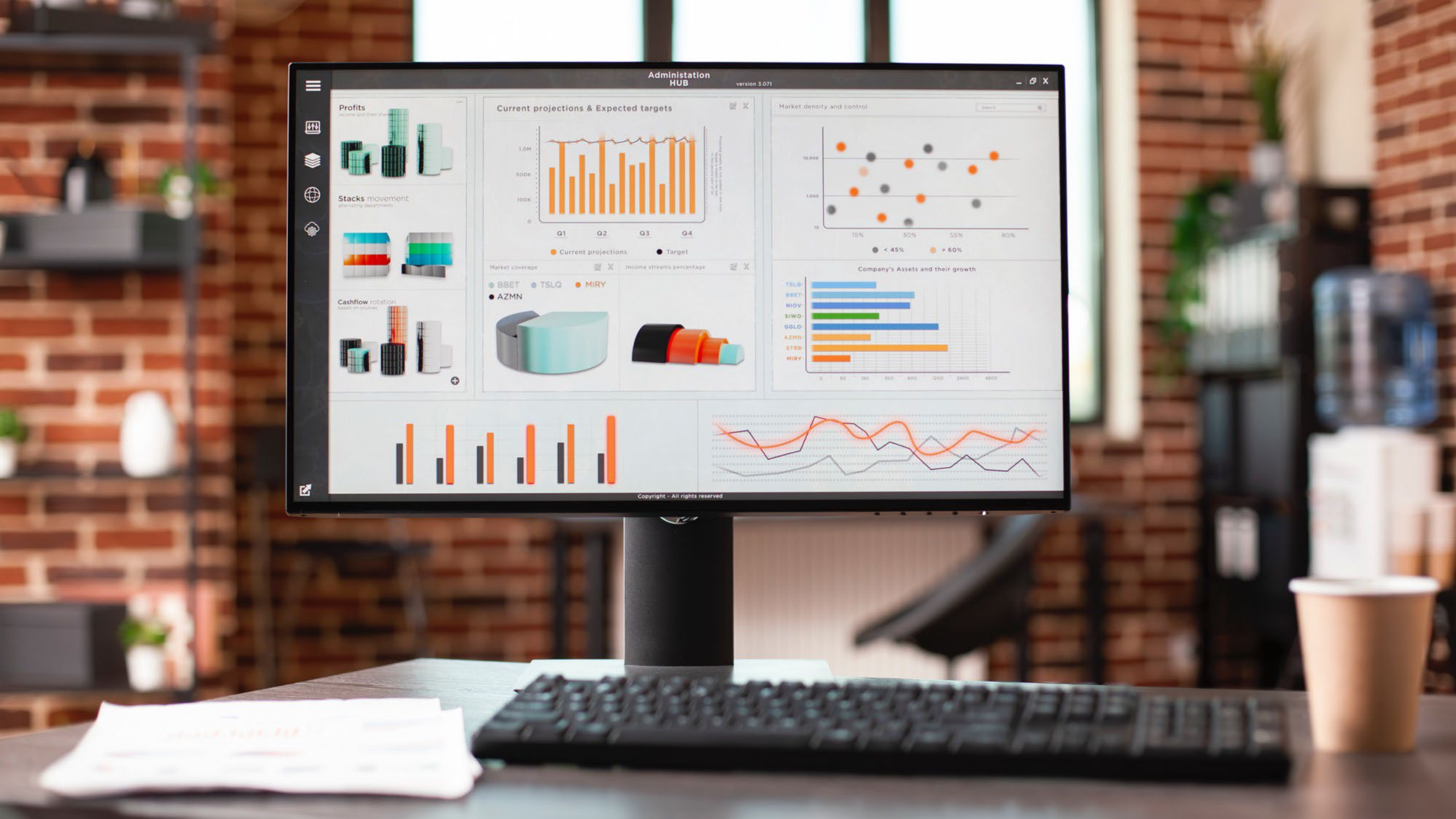


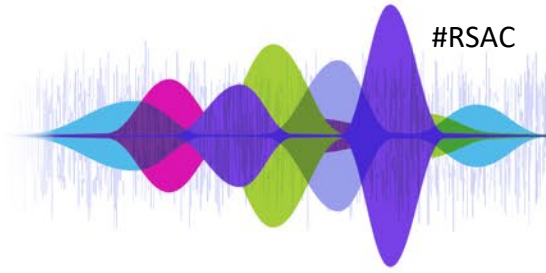
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.


Administation
HUB
version 3.071
Profits
Stacks movement
Cashflow rotation
Current projections & Expected targets
1.0M
500K
100K
0
Q1
Q2
Q3
Q4
Current projections
Target
Market density and control
10,000
1,000
10
15%
30%
55%
80%
< 45%
> 60%
Market coverage
BBET
TSLQ
MIRY
AZMN
Income streams percentage
Company's Assets and their growth
TSLQ
BBET
NIOV
SIWO
GGLO
AZMN
STRB
MIRY
Copyright - All rights reserved

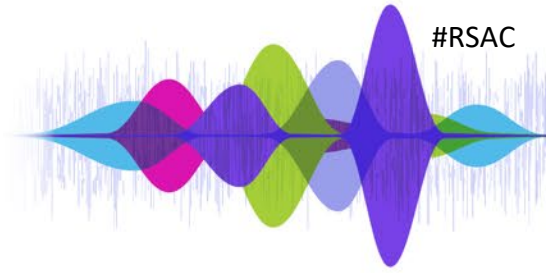


Problem Statements

- Cybersecurity teams want to clearly communicate risk to stakeholders
- Organizational leadership wants objective methods to quantify risk
- Sometimes it feels like we have too much data to report, sometimes it feels like we do not have enough
- Everyone is talking about automation like we should be doing it already

- **Two of the most common questions I am asked are:**
  - "What cybersecurity metrics should I report to my leadership?"
  - "Aren't there scripts, checklists, or KPIs I can download from somewhere?"

The Purpose of Cybersecurity Business Intelligence

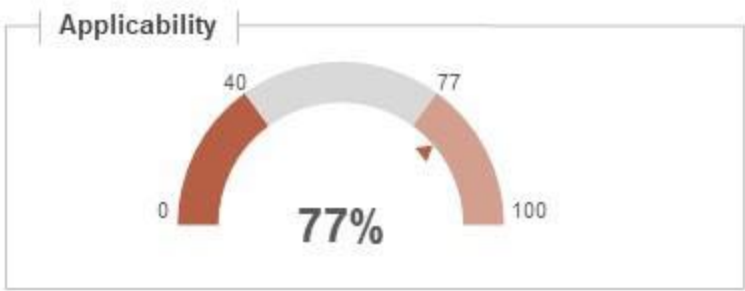


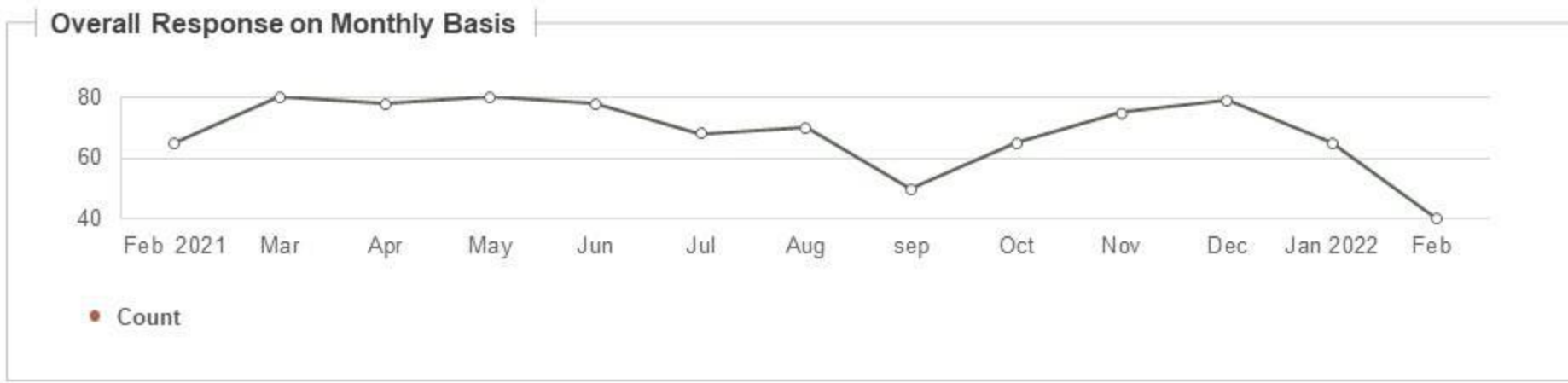
- "For all practical decision-making purposes, we need to treat measurement as observations that quantitatively reduce uncertainty."
  - Douglas W. Hubbard, How to Measure Anything in Cybersecurity Risk

- Ultimately, the goal of every cybersecurity team should be ***to enable the organization's technology systems to support the organization's mission***
- We can use business intelligence to measure the state of our cybersecurity safeguards, thus reducing the uncertainty around what we can control
- By reducing uncertainty, we can facilitate better business decisions

Dashboard to assess phishing awareness training program efficiency

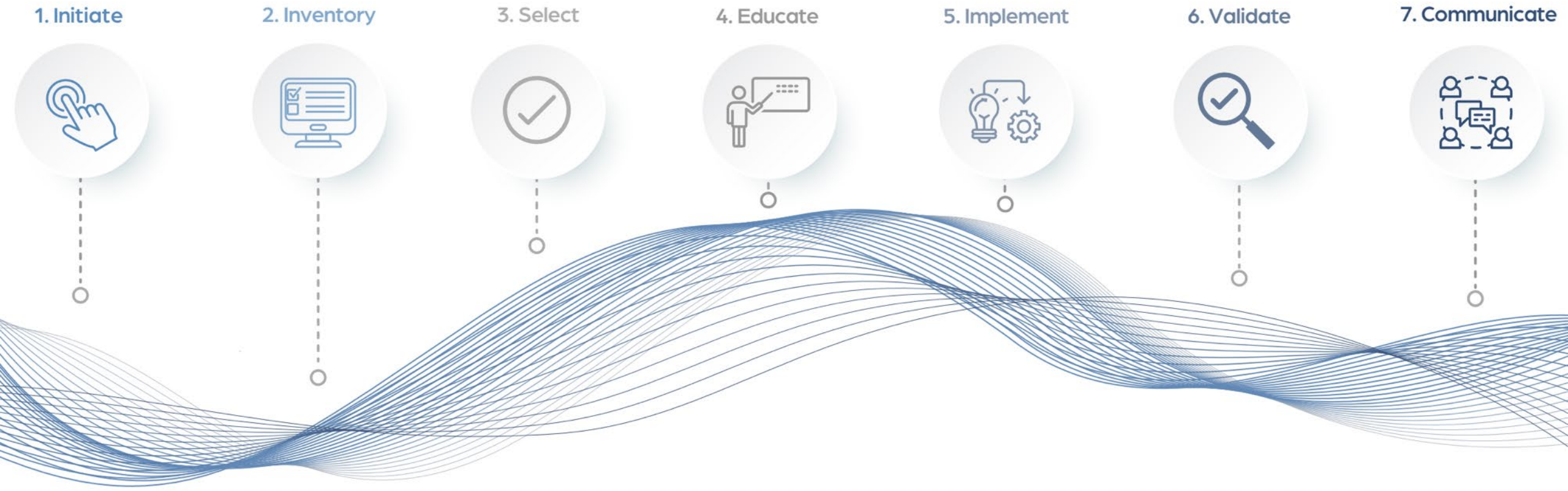
This slide covers KPI dashboard to assess phishing awareness training program efficiency. It involves details such as overall responses on monthly basis, employee satisfaction rate, net promoter score and major training courses.

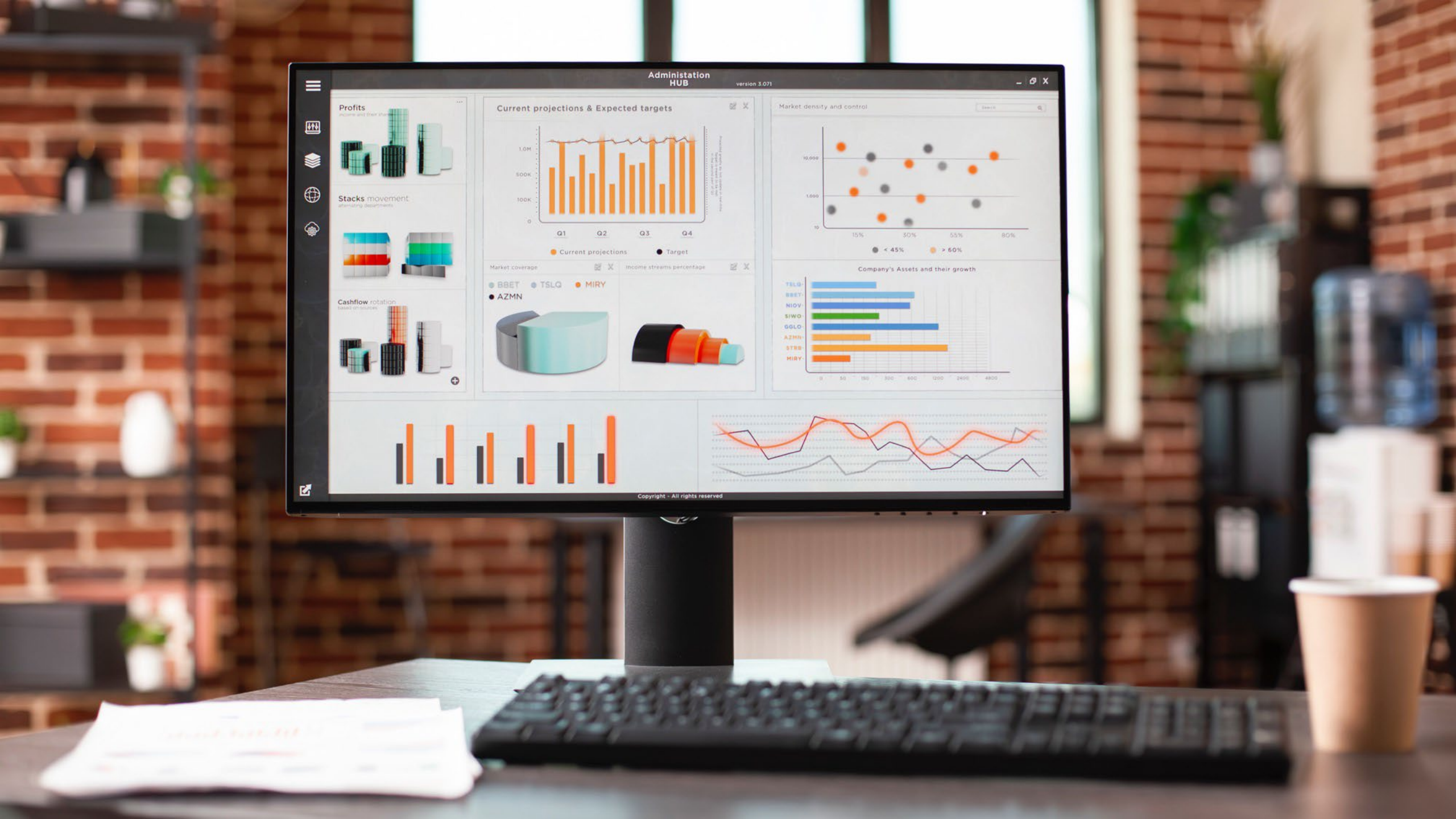




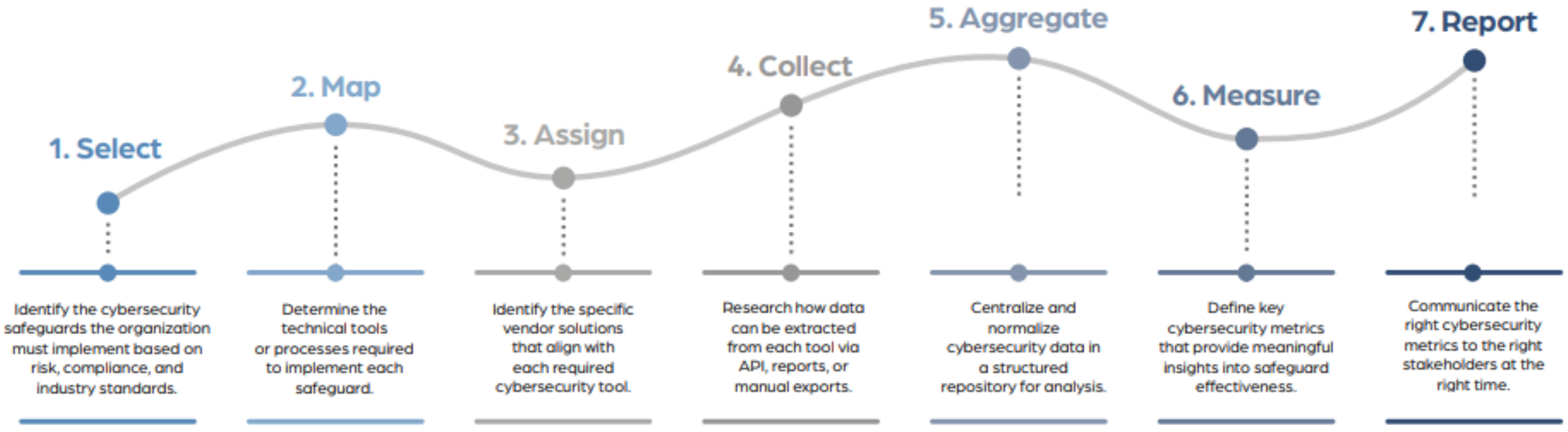
This graph/chart is linked to excel, and changes automatically based on data. Just left click on it and select "Edit Data".

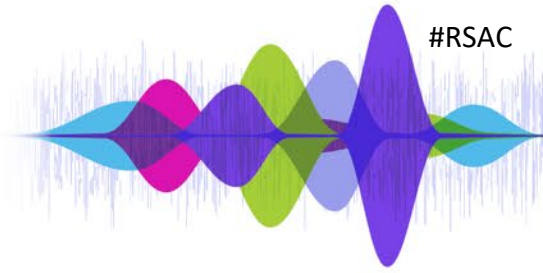
CRF Governance, Risk, Compliance (GRC) Roadmap




Administation
HUB
version 3.071
Profits
Stacks movement
Cashflow rotation
Current projections & Expected targets
1.0M
500K
100K
0
Q1
Q2
Q3
Q4
Current projections
Target
Market density and control
10,000
1,000
10
15%
30%
55%
80%
< 45%
> 60%
Market coverage
BBET
TSLQ
MIRY
AZMN
Income streams percentage
Company's Assets and their growth
TSLQ
BBET
NIOV
SIWO
GGLO
AZMN
STRB
MIRY
Copyright - All rights reserved

CRF Business Intelligence Model (BIM) Steps


1. Select
Identify the cybersecurity safeguards the organization must implement based on risk, compliance, and industry standards.
2. Map
Determine the technical tools or processes required to implement each safeguard.
3. Assign
Identify the specific vendor solutions that align with each required cybersecurity tool.
4. Collect
Research how data can be extracted from each tool via API, reports, or manual exports.
5. Aggregate
Centralize and normalize cybersecurity data in a structured repository for analysis.
6. Measure
Define key cybersecurity metrics that provide meaningful insights into safeguard effectiveness.
7. Report
Communicate the right cybersecurity metrics to the right stakeholders at the right time.

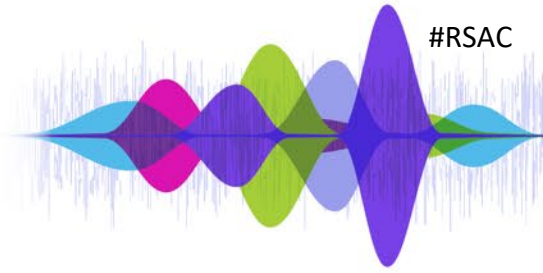


Step #1: Select Safeguards

- Before an organization can choose which metrics to track and automate, they must clearly identify which safeguards give them the best chance of success
- Too many organizations do not have a clearly defined plan
- Too many decide to follow “industry best practices” that are ever changing

- Organizations should work with their corporate counsel to formally decide:
  - Which safeguard libraries are required by laws and regulations?
  - Which safeguard libraries has the organization agreed to follow by contract?
  - Which safeguard libraries do they choose to follow to achieve their mission?

Step #1: Select Safeguards (Example)



- For example, consider the example of a California Bank, doing business with customers in the Midwest, New York, and Europe

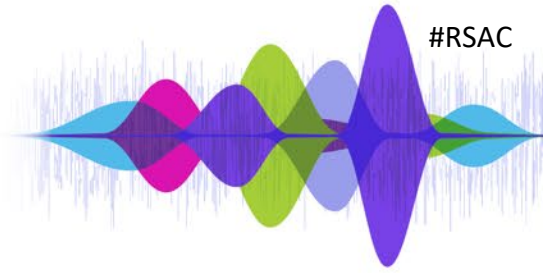
- ***By law***, they should consider safeguards defined by CCPA, NYDFS, & GDPR
- ***By contract***, they should evaluate the need to follow PCI, data breach notification, and cyber insurance requirements
- ***By choice***, they might choose to implement the NIST CSF

- Another option is to consider an aggregate safeguard library, that maps to each of these standards (such as the ***CRF Safeguards***)

Step #2: Map Tools

- First, an organization has clearly identified which safeguards they intend to implement
- Next, they must map each safeguard against the technical tool or business process they will use to implement the safeguard

- Technical safeguards are typically simple to map against technical tools
- Governance or operational safeguards may be more manual or map against documentation instead
- ***This mapping should then be de-duplicated to create one list***



Step #2: Map Tools (Example)

ID	Safeguard	Tool	Product
SYS-01	Maintain an Endpoint Detection and Response (EDR) system to detect and alert malicious activity on the organization's computing systems, whether onsite or remote.	Endpoint Detection & Response (EDR)	
SW-10	Maintain a software application control system on each organization's computing systems to ensure that only authorized software can execute.	Software Application Control	
VUL-01	Maintain a Vulnerability Management (VM) system to detect and track weaknesses in the organization's information systems.	Vulnerability Management (VM)	

Step #3: Assign Vendors

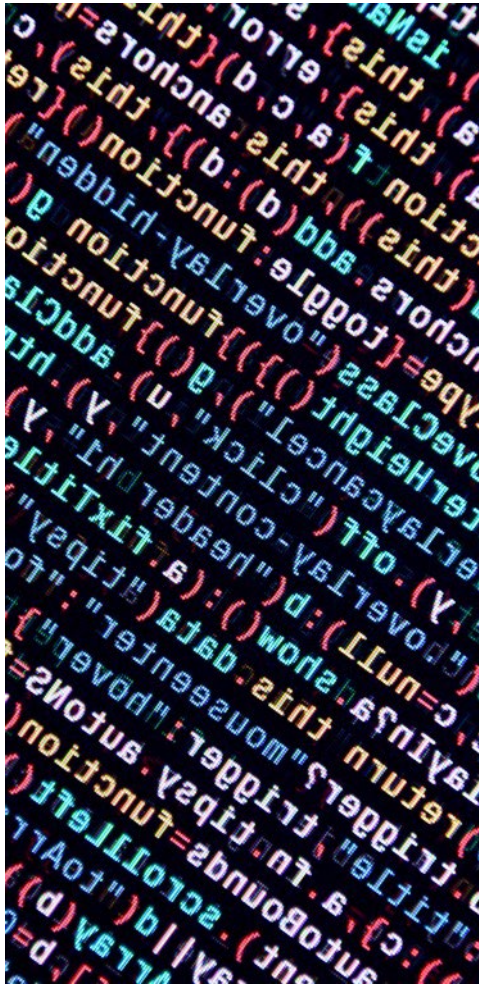
- The input to this next steps is a de-duplicated list of the cybersecurity tools they have (or plan) to implement
- Each tool or process in this list must be mapped against the specific vendor product they chose to implement
- Working through this exercise also helps an organization to create a cybersecurity enterprise architecture and evaluate their tool library
- Over time the safeguard library is less likely to change, but the tool library may evolve

Step #3: Assign Vendors (Example)

ID	Safeguard	Tool	Product
SYS-01	Maintain an Endpoint Detection and Response (EDR) system to detect and alert malicious activity on the organization's computing systems, whether onsite or remote.	Endpoint Detection & Response (EDR)	Crowdstrike Falcon
SW-10	Maintain a software application control system on each organization's computing systems to ensure that only authorized software can execute.	Software Application Control	ThreatLocker
VUL-01	Maintain a Vulnerability Management (VM) system to detect and track weaknesses in the organization's information systems.	Vulnerability Management (VM)	Tenable.io

Step #4: Collect Data

- At this point in the process, an organization should have a list of cybersecurity products and vendors that they have implemented
- Next, they should research whether each tool can be queried
- Ideally, each vendor would provide an API, but at times may only provide data download (via JSON, CSV, etc)



- Once an organization knows which vendors provide automated access to data, then they can research specifically which data fields are available

Step #4: Collect Data (Example)

CROWDSTRIKE

Platform Services Why CrowdStrike Learn Company

Docs / OpenAPI Docs

Docs

- CrowdStrike SDKs
- Foundry Samples
- Next-Gen SIEM
- OpenAPI Docs

OpenAPI Docs

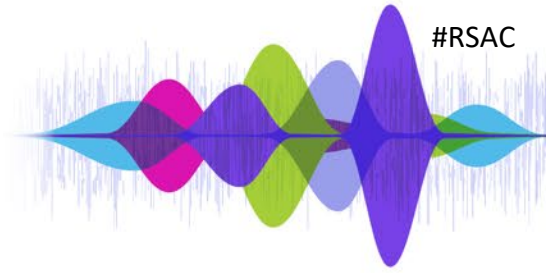
CrowdStrike's OpenAPI Specifications

Note
You must be logged into the Falcon console in order to access the OpenAPI specification and docs.

Cloud environment	API reference info link
US-1	https://assets.falcon.crowdstrike.com/support/api/swagger.html

- **Falcon Streaming — Stream detections and audit security events**
  With this API, users can monitor real-time events and receive alerts from their instances as they occur within a single data session, providing a low-latency, high-throughput data delivery mechanism.
- **Falcon Data Replicator — Ingest and correlate data**
  Falcon Data Replicator gives security teams the ability to export complete endpoint data from the Falcon agent to their environment for independent analysis. It provides customers with the means to ingest the data from the Falcon platform into their local data warehouse and correlate it with logs collected from other sources.
- **Falcon Threat Graph™ — Accelerate investigation by visualizing relationships**
  The Falcon Threat Graph API leverages CrowdStrike's multi-petabyte graph database to reveal the underlying relationships between indicators of compromise (IOCs), devices, processes, and other forensic data and events, such as files written, module loads, or network connections. Integration with visualization tools such as Maltego allows you to traverse the graph to investigate relationships between events.

Every vendor with an API will document the API and provide their customers documentation on the data that is accessible



Step #5: Aggregate

- Once an organization understands the data that is available, then they must aggregate the data into a place where it can be processed
- To get started, an organization can directly report against APIs
- In the long term, organizations will want the data where they can manage it
- Practically, many organizations choose to move the data to a staging database to clean and normalize before moving it to production for reporting
- Organizations often use CMDB, CAASM, or BI tools for this purpose

- We are often asked which tool is best for this step, and our answer is: ***the best tool is the tool you and your organization will consistently use!***

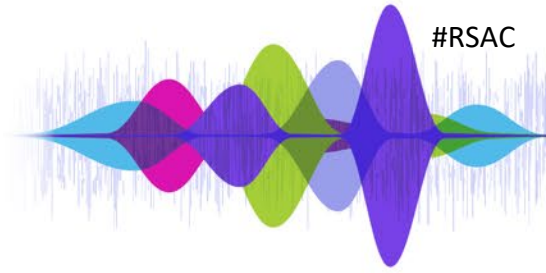
Step #5: Aggregate (Sample Databases)

Step #6: Measure

- Next, the organization can decide which KPIs or KRIs to report to the business
- This is the step where the organization can finally create the dashboards and automated reports they've been dreaming about
- Likely these scores will be a combination of aggregate maturity ratings and measures of specific KPIs relevant to the business

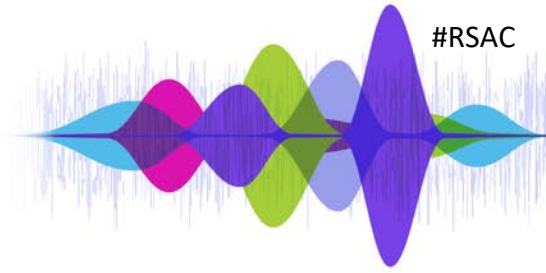
- Remember, ***prioritized safeguards lead to prioritized metrics***

Step #7: Report



- The purpose of the final step is to put data into stakeholders' hands so they can use that information to reduce uncertainty and make better decisions
- Provide KPIs to stakeholders that matter to them on a cadence that facilitates better decision making
- The higher someone is in an organization, the more aggregate the ratings
- The more hands on the stakeholder is, the more tactical the data will be
- **General guidelines:**
  - Senior Leadership – Quarterly to annual reporting, 10-20 minutes each
  - Tactical Leadership – Weekly to monthly reporting, 30-60 minutes minimum each

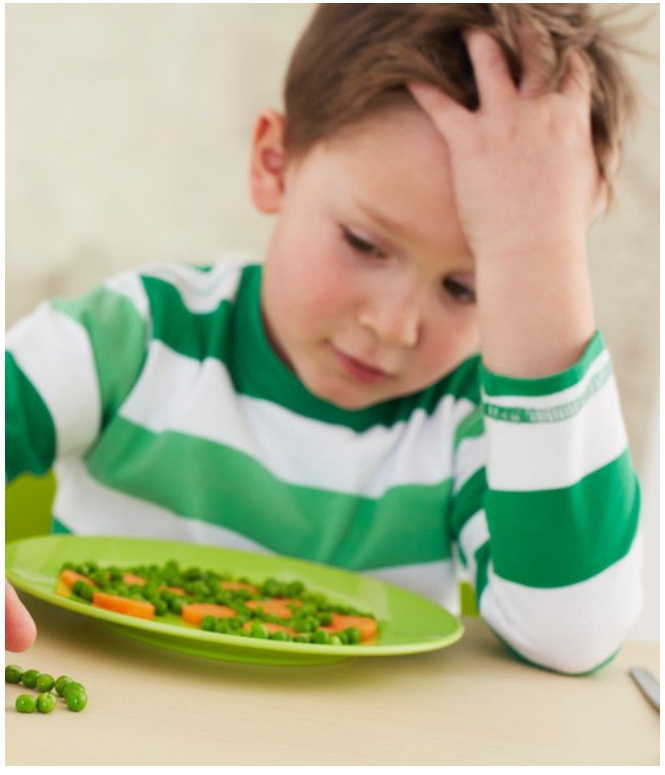
Reporting Cybersecurity Risk to Senior Leadership



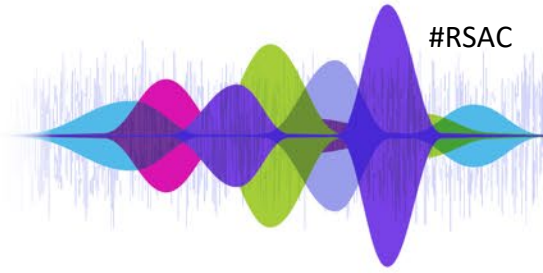
- The SANS Institute conducted a survey to determine what senior leadership expects from their cybersecurity teams.
- Alan Paller and John Pescatore presented their findings in a SANS webcast (https://sans.org/webcasts)
- Primarily, the survey showed that senior leadership wants:
  - To trust their cybersecurity leadership advisors.
  - To know that their cybersecurity team is competent and addressing risk.
  - To know they are defending their information systems at least as much as their peers.
  - To have an efficient cybersecurity team that does not cost too much.
- Ultimately, leadership wants to know that their cybersecurity team is addressing cybersecurity risk so they do not need to think about it.

Practical Considerations / Realities

- As an organization, you must walk before you can run
- The first step cannot be a dashboard, or even metrics



- ***Start by defining your target state, which cybersecurity safeguards you believe will help you achieve your mission***
- Then you can decide how to map safeguards, to tools, to vendors, to APIs
- Continuous monitoring is a worthy target, but first you must eat your vegetables



“Apply” Slide – Making this Even More Practical

1. Be definitive about your goals – decide specifically which cybersecurity safeguards you believe will help you achieve your mission
2. Be self-aware, regularly assess the status of the safeguards you choose
3. Start small, aggregate small amounts of data with BI tools, then progress to larger, more comprehensive systems
4. Learn to tell leadership the story they need to hear

Next Steps to Learn More

Resources for Further Study:

- Cybersecurity Risk Foundation – Business Intelligence Model (BIM)
  - (https://crfsecure.org/)

- The Information Diet, Clay A. Johnson
- Storytelling with Data, Cole Nussbaumer Knaflic

- SANS LDR419: Performing A Cybersecurity Risk Assessment
- SANS LDR519: Cybersecurity Risk Management and Compliance

Ask James Tarala on LinkedIn:

RSAC™ 2025 Conference

Many Voices.
One Community.